

THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,)	No. CR19-159-RSL
)	
Plaintiff,)	
)	PAIGE THOMPSON’S MOTION FOR
v.)	A NEW TRIAL
)	
PAIGE A. THOMPSON,)	
)	
Defendant.)	

I. INTRODUCTION

Paige Thompson, through counsel, moves for a new trial on Counts 1–2 and 4–7 of the Second Superseding Indictment pursuant to Rule 33 of the Federal Rules of Criminal Procedure. Those counts charged Ms. Thompson with wire fraud (Count 1) and with violations of the Computer Fraud Abuse Act (“CFAA”) (Counts 2 and 4–7). The government dismissed Count 3,¹ she was convicted on Counts 1–2 and 4–8, and the jury acquitted her of the remaining counts, which related to alleged identify theft, Counts 9–10. (Dkt. 355.)

This motion is brought under Rule 33 because “the interest of justice so requires.”² The Supreme Court’s decision in *Ruan v. United States*, 597 U.S. ___, 142

¹ The dismissal is noted on the docket as happening on June 9, 2022, although there is no docket number.

² This motion does not address Count 8, which charges a different subsection of the CFAA from Counts 2 and 4–7.

1 S. Ct. 2370 (2022), rendered ten days after the jury verdicts in this case, makes clear as
 2 a matter of statutory interpretation that the *mens rea* element contained in the CFAA
 3 not only required the government to prove for Counts 2 and 4–7 that Ms. Thompson
 4 *intentionally* accessed a computer but that she also *intentionally* did so “without
 5 authorization.” The Court’s jury instructions as to those counts were—at a minimum—
 6 ambiguous as to whether the “intentionally” *mens rea* utilized in the instruction applied
 7 both to the elements of “without authorization” and to “access.” This was error under
 8 *Ruan*. And it tainted not only the convictions for Counts 2 and 4–7, but also the wire
 9 fraud conviction on Count 1 since it hinged upon the CFAA’s “without authorization”
 10 element.

11 The Court should grant Ms. Thompson a new trial.

12 **II. PROCEDURAL HISTORY AND BACKGROUND**

13 The government charged Ms. Thompson in the Second Superseding Indictment
 14 with wire fraud (Count 1), computer fraud and abuse under the CFAA (Counts 2 and 4–
 15 8), access device fraud, and aggravated identity theft (Counts 9 and 10). (Dkt. 166 at 6–
 16 9.) Both the wire fraud and CFAA counts alleged the same basic pattern of conduct:
 17 unauthorized access and damage.

18 Count 1 charged that Ms. Thompson “exploit[ed] . . . misconfigured web
 19 application firewalls” to obtain “stolen credentials to access and copy [] data” stored on
 20 AWS servers (*i.e.*, unauthorized access) and to utilize those servers to “mine
 21 cryptocurrency” (*i.e.*, damage). (Dkt 166 at 3.) Additionally, Count 1 asserted that the
 22 manner in which Ms. Thompson accessed the AWS servers “implicitly represented”
 23 that her commands “were legitimate commands sent by users with permission to send
 24 such commands, rather than commands sent by a person who had stolen the security
 25 credentials and who lacked authority to use the accounts and roles and send the
 26

1 commands.” (*Id.* at 4.) Thus, authorization—or Ms. Thompson’s alleged lack thereof—
 2 was central to Count 1.

3 Counts 2 and 4 through 7 charged Ms. Thompson with “intentionally access[ing]
 4 a computer without authorization” and “thereby obtain[ing] information” in violation of
 5 the CFAA. (*Id.* at 6–7.) Count 8 alleged Ms. Thompson “knowingly caused the
 6 transmission of a program, information, code, and command . . . and, as a result of such
 7 conduct, intentionally caused damage without authorization to protected computers” in
 8 violation of the CFAA. (*Id.* at 8.)

9 Ms. Thompson’s trial started on June 6, 2022, and closing arguments and the
 10 Court’s instructions to the jury took place on June 15, 2022. In its instructions regarding
 11 the CFAA counts (Counts 2 and 4–7), the Court instructed the jury that the government
 12 had to prove beyond a reasonable doubt that on or about, or between, certain dates:

13 *First*, [] the defendant intentionally accessed without authorization a
 14 computer;

15 *Second*, by accessing without authorization a computer, the defendant
 16 obtained information contained in a financial record of a card issuer; and

17 *Third*, the value of the information obtained exceeded \$5,000.

18 A person accesses a computer “without authorization” when (1) the
 19 computer is protected by a generally applicable rule regarding access
 20 permissions, such as a username and password requirement, credential
 21 requirement, or other authentication system that prevents the general
 22 public from accessing the computer, and (2) the person circumvents that
 23 rule regarding access permissions to gain access to the computer.

24 (Dkt. 330 at 20–24 (emphasis added).)

25 The instructions for Counts 2 and 4–7 do not make clear whether the subjective
 26 intent of the defendant—the “intentionally” *mens rea*—applies solely to the defendant’s
 access of the computer or to both the access of the computer and the lack of
 authorization. Further, the Court’s definition of “without authorization” does not

1 require the person to access the computer with any level of *mens rea* at all and the word
2 “intentionally” is completely missing from the definition.³

3 The government’s theory on those counts and the wire fraud charge did not
4 center solely on Ms. Thompson’s subjective intent, but also on the subjective intent of
5 the companies whose rented servers she accessed. During closing argument, on June 17,
6 2022, the government told the jury:

7 The defense is trying to convince you that it doesn’t matter that these
8 companies didn’t want their data downloaded, that it didn’t matter that
9 they tried to protect it, that it didn’t matter that they didn’t want these
10 credentials to be used this way, and they didn’t know that their web
facing applications were talking to an internal resource. Guess what? It
does matter. It matters a lot.

11 (6/17/22 Tr. at 94.) The defense’s theory, in contrast, was that the alleged victims’
12 subjective intent in programming their web application firewall interfaces was
13 irrelevant because it had no bearing on whether Ms. Thompson’s access of those
14 interfaces was “without authorization” as that term is defined in the CFAA nor whether
15 Ms. Thompson subjectively intended to access those interfaces “without authorization.”

16 In urging the jury to reject the defense’s theory in closing rebuttal, the
17 government went further and told the jurors not to “buy into this hyper-technical
18 argument that a machine executing commands by itself is authorization[,]” but instead
19 to use the “common meaning” of authorization, like finding a spare house key under a
20 doormat. (6/16/2022 Tr. at 93–94.) The government’s sleight of hand here—by
21 focusing on the alleged victims’ claimed intent, rather than Ms. Thompson’s subjective
22 intent, removed the *mens rea* element as to “without authorization” from the CFAA and
23

24 ³ This makes sense given that the Court’s definition of “without authorization” is taken,
25 in part, from the Ninth Circuit’s decision in *hiQ*, a civil tortious interference matter on
26 appeal from a temporary restraining order proceeding that had no necessity to prove
criminal *mens rea*. See *hiQ Labs, Inc. v. LinkedIn, Corp.*, 31 F.4th 1180, 1201 (9th Cir.
2022).

the wire fraud statute. And, unfortunately, this sleight of hand was not cured by the Court’s instructions to the jury because they did not make crystal clear—in the manner that *Ruan* now requires—that the government was bound to prove not only that Ms. Thompson intentionally accessed the computers in question, but that she also intentionally acted “without authorization.” This confusion was compounded by the fact that the Court’s definition of “without authorization” also lacked the word “intentionally.” Because it is possible that the jury understood the “intentionally” *mens rea* requirement as used in Instruction Nos. 18–22 as applying solely to the “accessed” element and not to the “without authorization” elemental clause, a new trial is warranted with a set of jury instructions that comport with *Ruan*.

On June 17, 2022, following closing arguments and after being given the instructions above, the jury convicted Ms. Thompson of the wire fraud and CFAA counts (Counts 1–2 and 4–8) and acquitted her on the access device fraud and aggravated identity theft counts (Counts 9–10). (Dkt. 355.) Ten days later, on June 27, 2022, the Supreme Court’s decision in *Ruan* was issued.

III. ARGUMENT

A. This Court has broad discretion to grant a new trial and should use its discretion here to correct a serious miscarriage of justice.

Under Rule 33, “upon the defendant’s motion, the [C]ourt may vacate any judgment and grant a new trial if the interest of justice so requires.” The Court’s “power to grant a motion for a new trial is much broader than its power to grant a motion for judgment of acquittal.” *United States v. Alston*, 974 F.2d 1206, 1211 (9th Cir. 1992). A district court need not view the evidence in the light most favorable to the verdict; it may weigh the evidence and evaluate the credibility of the witnesses in that process. *Id.* Moreover, “[i]f the [district] court concludes that . . . the evidence preponderates sufficiently heavily against the verdict that a serious miscarriage of justice may have

1 occurred,” it may set aside the verdict and grant a new trial even “despite the abstract
 2 sufficiency of the evidence to sustain the verdict.” *Id.* at 1211–12; *see also United*
 3 *States v. Bays*, 995 F.2d 233, 233 (9th Cir. 1993).

4 Here, in the wake of *Ruan*, the evidence “preponderates sufficiently heavily
 5 against the verdict” because the jury instructions were insufficiently clear to ensure that
 6 the jury properly understood the government needed to prove beyond a reasonable
 7 doubt not only that Ms. Thompson intentionally accessed the computers, but that she
 8 did so intentionally “without authorization” given the way the computers were
 9 structured. *See Ruan*, 142 S. Ct. at 2376 (“[T]he [g]overnment must prove beyond a
 10 reasonable doubt that the defendant knowingly or intentionally acted in an unauthorized
 11 manner.”). This lack of clarity was particularly problematic here because the
 12 government argued that the jury should ignore “hyper-technical” definitions of “without
 13 authorization” in favor of focusing on the alleged victims’ subjective intent in designing
 14 their web application firewall interfaces. (*See* 6/17/22 Tr. at 94 (government arguing
 15 that the alleged victims’ intent “matters a lot.”)).

16 The government’s choice to refocus the jury on the alleged victims’ purported
 17 intent instead of Ms. Thompson’s subjective intent circumvents the Supreme Court’s
 18 instruction that the term “authorization” under the CFAA is a “gates-up-or-down
 19 approach” that depends solely on the actions taken by the relevant computer system, not
 20 the owner’s intent. *Van Buren v. United States*, 141 S. Ct. 1648, 1659 (2021); *see LVRC*
 21 *Holdings LLC v. Brekka*, 581 F.3d 1127, 1134–35 (9th Cir. 2009). This understanding
 22 of “authorization” comports with the understanding of that term in the tech community,
 23 of which Ms. Thompson was a member. *See Van Buren*, 141 S. Ct. at 1658 n.9 (quoting
 24 A Dictionary of Computing’s definition of “authorization” as a “process by which
 25 users, having completed an . . . authentication stage, gain or are denied access to
 26 particular resources based on their entitlement”). The relevant question is not what the

1 alleged victims intended in setting up their web application firewalls—their gates—it is
 2 what Ms. Thompson understood and intended when she came across those gates and
 3 they were wide open. This was not clear from the jury instructions for Counts 2 and 4–7
 4 as given in light of *Ruan*, particularly when compounded with the government’s closing
 5 arguments and focus on the alleged victims’ claimed intent. A new trial is thus
 6 necessary.

7 **B. Under *Ruan*, the government would not only have needed to prove**
 8 **beyond a reasonable doubt that Ms. Thompson intentionally accessed**
 9 **a computer, but that she intentionally did so without authorization.**

10 *Ruan*, which was published ten days after the jury verdicts in this case, is
 11 directly analogous⁴ and makes clear as a matter of statutory interpretation that the
 12 “intentionally” *mens rea* element contained in the CFAA not only required the
 13 government to prove beyond a reasonable doubt for Counts 2 and 4–7 that
 14 Ms. Thompson intentionally accessed a computer, but that she also intentionally did so
 15 “without authorization.” 142 S. Ct. 2370. The statute addressed in *Ruan*, 21 U.S.C.
 16 § 841, like the CFAA, contains a general scienter provision— “knowingly or
 17 intentionally.” *Id.* at 2375. The statute also contains an authorization exception that
 18 precedes that scienter provision making it unlawful, “[e]xcept as authorized[,] . . . for
 19 any person knowingly or intentionally . . . to manufacture, distribute, or dispense . . . a
 20 controlled substance.” *Id.* at 2376 (quoting 21 U.S.C. § 841). The Supreme Court in
 21 *Ruan* held as a matter of statutory interpretation that § 841’s “knowingly or

22 ⁴ Although some of the discussion in *Ruan* relates to burden-shifting, that aspect of the
 23 decision regarding the Comprehensive Drug Abuse and Prevention and Control Act is
 24 not relevant to the CFAA. In prosecutions under 21 U.S.C. § 841 for knowingly or
 25 intentionally distributing a controlled substance “except as authorized,” a separate
 26 section places a special burden of production as to “any [] exemption or exception” in
 the statute on the person claiming its benefit. 21 U.S.C. § 885(a)(1); *see Ruan*, 142
 S. Ct. at 2380. Here, in contrast, the burdens of both production and persuasion remain
 on the government.

1 intentionally” *mens rea* applied to the elemental authorization exception clause and thus
2 that “the [g]overnment must prove beyond a reasonable doubt that the defendant
3 knowingly or intentionally acted in an unauthorized manner.” *Id.* Because the *Ruan*
4 decision is one of statutory interpretation, it is fully retroactive. *See United States v.*
5 *Aguilera-Rios*, 769 F.3d 626, 631 (9th Cir. 2014) (stating that “[d]ecisions of statutory
6 interpretation are fully retroactive because they do not change the law, but rather
7 explain what the law has always meant.”).

8 In so holding, the Supreme Court rejected the government’s concern that a
9 subjective scienter requirement for “authorization” would allow “bad-apple doctors to
10 escape liability,” and explained that often a lack of authorization is “what separates
11 wrongfulness from innocence.” *Ruan*, 142 S. Ct. at 2377. Similarly, here the
12 government argued that Ms. Thompson’s “hyper-technical” defense would result in “no
13 such thing as computer hacking.” (6/16/22 Tr. at 57, 93.) But as *Ruan* made clear “[t]his
14 kind of argument, however, can be made in many cases imposing scienter requirements,
15 and we have often rejected it[.]” 142 S. Ct. at 2382. It is also patently untrue; there are
16 any number of cases dealing with hackers who intentionally access a computer system
17 and know they lack the authorization to do so. In *United States v. Phillips*, for example,
18 the defendant used code to automatically guess Social Security numbers to steal
19 information from a known computer system (an approach known as a “brute force
20 attack”) after being asked repeatedly to stop by the computer system’s owner. 477 F.3d
21 215, 218 & n.2, 219 (5th Cir. 2007).

22 Ms. Thompson, by contrast, accessed open forward proxies whose operators
23 were unknown to her at that time with no concrete evidence of why those proxies were
24 left open or set to forward commands from outside the AWS environment. (*See, e.g.,*
25 6/13/22 Tr. at 39; 6/15/22 Tr. at 70–71.) Further, there was no evidence, on the few
26 occasions Ms. Thompson received an error message stating a particular command was

1 “unauthorized or forbidden,” that she circumvented those closed gates. (6/15/22 Tr. at
 2 71–72 (Professor Halderman testifying there was no “evidence she tried to go past that
 3 point” or “somehow override those places.”).) In other words, there was no evidence
 4 that Ms. Thompson *intentionally* circumvented a generally applicable rule regarding
 5 access permissions to gain access to the alleged victims’ computer systems. (*See*
 6 Dkt. 330 at 20–25.) There was also no evidence that the computers were password
 7 protected or otherwise prevented a member of the public from viewing the information.
 8 The government attempted to fill this evidentiary void with the intent of the alleged
 9 victims in setting up the access permissions for their computer systems, but that is
 10 misleading and improper, especially in the wake of *Ruan*. *See* 142 S. Ct. at 2382
 11 (stating that the government may point to the *unreasonableness* of a defendant’s
 12 subjective belief that he or she was authorized, as measured against objective standards,
 13 to help carry the burden of proving the *mens rea* element) (quoting *Cheek v. United*
 14 *States*, 498 U.S. 192, 203–04 (1991)).

15 **C. The Court’s CFAA jury instructions as to Counts 2 and 4–7 did not**
 16 **make clear to the jury the government’s burden to prove that**
 17 **Ms. Thompson intentionally acted without authorization; a new**
 18 **instruction must be utilized to comport with *Ruan*.**

19 Counts 2 and 4–7 instructions given pre-*Ruan* were—at a minimum—ambiguous
 20 as to whether the “intentionally” *mens rea* requirement applied both to the statutory
 21 elements of “without authorization” and “access.” Without the explicit burden of
 22 having to prove Ms. Thompson’s subjective intent as to authorization, the government
 23 felt free to argue that proving that Ms. Thompson “intentionally accessed a computer
 24 without authorization” turned on the alleged victims’ claimed intent to exclude her
 25 access, rather than on an inquiry as to her subjective intent regarding authorization
 26 when she accessed the computers. After *Ruan*, the only remedy for this error is a new
 trial.

1 During such new trial, the jury instructions regarding Counts 2 and 4–7 of the
 2 CFAA charges must be changed to comport with *Ruan*. Those instructions should
 3 provide as follows (with the statutory elements required by *Ruan* highlighted and
 4 emphasized):

5 The defendant is charged in Count [] of the indictment with [unlawfully
 6 obtaining information of [] in violation of Section 1030(a)(2) of Title 18
 7 of the United States Code] [transmitting a program, information code, or
 8 command to a computer, intending to cause damage, in violation of
 9 Section 1030(a)(5) of Title 18 of the United States Code]. For the
 defendant to be found guilty of that charge, the government must prove
 each of the following elements beyond a reasonable doubt:

10 *First*, [between/beginning] on or about [], the defendant ***intentionally***
 11 [accessed a computer] [caused the transmission of a program,
 information, code, or command to a computer];

12 *Second*, the defendant ***intentionally*** did so without authorization;

13
 14 *Third*, [by accessing without authorization a computer, the defendant
 15 obtained information contained in a financial record of a card
 16 issuer/obtained information from a computer that was used in or affecting
 17 interstate or foreign commerce or communication] [as a result of the
 transmission, the defendant intentionally impaired the integrity or
 availability of data, a program, a system, or information]; and

18 *Fourth*, the value of the information [obtained][lost] exceeded \$5,000.

19 A person accesses a computer, quote, without authorization when (1) the
 20 computer is password protected or otherwise prevents a member of the public
 21 from viewing the information, and (2) the person ***intentionally*** circumvents the
 22 computer's generally applicable rules regarding access permission to gain access
 to the computer.

23 (Dkt. 330 at 20–24 (modified and emphasis added).)⁵

24
 25
 26 ⁵ The definition of “without authorization” is the one Ms. Thompson requested with the
Ruan inclusion of “intentionally.” (6/15/2022 Tr. at 132.)

1 In addition and as further supported by *Ruan*, the defense requests that the Court
 2 provide the mistake of law instruction the defense proposed (and the Court rejected)
 3 with the addition of the word “intentionally” before “act without authorization, (6/15/22
 4 Tr. at 134–36). These revised instructions make clear that the government must prove
 5 Ms. Thompson’s *mens rea* beyond a reasonable doubt both as to access and as to
 6 accessing “without authorization.”

7 **D. The failings of the jury instructions on Counts 2 and 4–7 also require**
 8 **a new trial on Count 1, the wire fraud charge.**

9 The failure to require that the government prove that Ms. Thompson intended to
 10 act “without authorization” taints not only the convictions on Counts 2 and 4–7, but
 11 also the wire fraud conviction on Count 1 as well. This is because the Second
 12 Superseding Indictment makes clear that the wire fraud count hinges on Ms.
 13 Thompson’s alleged lack of authorization. The government’s theory of wire fraud was
 14 that Ms. Thompson implicitly misrepresented that she had authorization to send
 15 commands to the alleged victims’ computer systems when she did not. (Dkt. 166 at 4;
 16 see 6/16/22 Tr. at 42–43 (government arguing at closing that “[o]nce she has the
 17 credentials, she uses them to gain the data, to gain access to do the cryptojacking. And
 18 in doing that, in using those credentials, she is representing that she is a person who
 19 should have those credentials, that she is a legitimate user of those credentials. She has
 20 to be a legitimate user for that to work, and so she is representing that, and that’s the
 21 trickery, that’s the misrepresentation.”).)

22 To convict Ms. Thompson of the Counts 2 and 4–7, the jury agreed she
 23 “intentionally accessed without authorization a computer” without authorization”
 24 without ever making a specific finding that she intentionally acted without authorization
 25 and, by extension, that she impliedly misrepresented her authorization for the wire
 26 fraud count. (See Dkt. 330 at 20–25.)

Although the wire fraud instruction defined “knowingly” as when “the defendant is the aware of the act and does not act through ignorance, mistake, or accident,” this definition did not eradicate the ambiguity—and potential juror confusion—created by the failure of the jury instructions to require the lack of authorization to be intentional. In fact, it may have made them even more impermissibly confusing. The convictions are thus invalid under *Ruan*.

Lastly, Ms. Thompson’s alleged statements, which the government offered into evidence at trial (and other government evidence of her purported intent at trial), do not change the overall analysis under *Ruan* for Counts 1–2 and 4–7 because the government always bore the burden of proof to establish that Ms. Thompson acted intentionally without authorization. At a minimum, the government’s repeated invocation of the alleged victims’ purported intent on this issue—rather than Ms. Thompson’s subjective intent—created an ambiguity in the jurors’ minds and the interests of justice require a new trial.

IV. CONCLUSION

Ms. Thompson respectfully requests, based on the foregoing, that her convictions on Counts 1–2 and 4–7 be vacated and that she be granted a new trial pursuant to Rule 33.

Respectfully submitted this 5th day of August 2022.

s/ Mohammad Ali Hamoudi
s/ Nancy Tenney
 Federal Public Defender’s Office

s/ Brian Klein
s/ Melissa Meister
 Waymaker LLP

Attorneys for Paige Thompson